学校编码：10384　　分类号＿＿＿密级＿＿

学号：X2008230016　　UDC ＿

厦门大学

硕　士　学　位　论　文

统一身份认证系统的设计与实现

Design and Implementation of Unified Identity Authentication System

洪素燕

指导教师姓名：　林坤辉　教授

专　业　名　称：　软　件　工　程

论文提交日期：2010　年　8　月

论文答辩时间：2010　年　　月

学位授予日期：2010　年　　月

答辩委员会主席：＿＿＿＿

评　　阅　　人：＿＿＿＿

2010 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

随着当今信息技术的日新月异，企业信息化建设步伐也在加快脚步，对各种应用系统的应用重视程度也在不断的提高，对企业提高工作效率和管理水平做出了巨大的贡献。在各种应用系统得到迅速发展的同时，由于这些应用系统的开发时期、运行平台、使用的技术各不相同，每个应用系统又有独立的身份验证机制，各应用系统分散登录，分散管理，如果不建立统一的身份认证系统，实现单点登录，势必造成企业的工作人员在实际工作中需要频繁的在各个应用系统中不断的登录和注销，严重影响了企业的工作效率。因此，建立一个统一的身份认证系统，不仅能方便用户的登录，提高工作效率，而且能保证各个系统的安全性。

针对目前企业信息系统应用服务多、跨越不同的开发平台、使用多种语言实现的特点，对现在流行的统一身份认证的模型进行了详细的分析和比较，结合身份认证模型的基础理论和企业应用的实际情况，构造了适合企业现阶段状况的单点登录模型，并根据设计给出了一个详细的实现。该系统充分考虑了目前企业应用服务的实际要求，具有良好的灵活性、可扩展性和跨平台性，实现了用户的统一身份认证。对企业的统一身份认证系统的建设具有一定的积极意义。

本文以厦门某公司企业信息化的实际建设情况为背景，探讨统一身份认证建设的需求、原则，讨论了项目所涉及的关键技术，具体的统一身份认证规划设计，统一身份认证系统的设计与实施。文章重点阐述了部署统一身份认证的情况，从统一身份认证的体系结构、认证流程几方面阐述了统一身份认证系统的设计，详细介绍在企业中部署统一身份认证系统的实施方案。

关键词：身份认证；目录服务；

Abstract

With the development of science and technology, the pace of informatization of enterprises has speeded up. The emphasis on the application of different utility systems has increased. And the informatization has made great contributions to the rise of work efficiency and management level of the enterprises. The utility systems have developed rapidly. At the same time, these systems have different development period, running platform, and technologies, and each system has an independent authentication mechanism, as well as an independent entry system and independent management, so if not establishing a unified identification system, the employees of the enterprises have to log in and log off to the different utility systems during work. This will have a bad impact on the efficiency. Therefore, establishing a unified identification system could not only facilitate the log in of the users, increase the efficiency, but ensure the security of the systems as well.

Now, the enterprises have the characteristics of having many information system application services, spanning different development platforms, using different languages. Because of these characteristics, it has detailed analysis and comparison of the modern unified identification model. Combined with the basic theories of identification model and the actual conditions of the application of the enterprises, it develops a unified identification system which is suitable for the actual conditions of the enterprises and provides a detailed realization according to the design. This system takes the actual requirements of the application service of the enterprises into account. It has great flexibility, extensibility and cross-platform, realizing the unified identification system of the users. It has active effect on the establishment of the unified identification system of the enterprises.

This thesis takes the actual establishment situation of informatization of a company in Xiamen, discussing the requirements and principles of the establishment of unified identification, as well as the key techniques in this program, the plan for unified system, the realization of catalogue services and systematic deployment. This thesis states the design of unified identification system and the situation of deploying

unified identification from the points of structure of unified identification, certification process, and catalogue design.

Key Words: Identity Authentication；LDAP；

目　录

第一章 绪 论 1

1.1 研究背景及意义 1

1.2 国内外研究状况概述 2

1.3 论文的主要内容和组织结构 3

第二章 身份认证相关技术 5

2.1 密码学 5

2.1.1 对称密钥算法 6

2.1.2 非对称密钥算法 7

2.1.3 其他加密算法 8

2.2 身份认证 9

2.2.1 身份认证定义 9

2.2.2 身份认证的方法 9

2.2.3 身份认证的意义 12

2.3 LDAP 协议 12

2.3.1 LDAP 简介 12

2.3.2 LDAP 四种基本模型 13

2.3.3 LDAP 的安全性 15

2.3.4 LDAP 的特点与优势 15

2.4 几种典型的单点登录模型研究 16

2.4.1 Broker-Based 模型 17

2.4.2 Agent-Based 模型 18

2.4.3 Agent and Broker-based 模型 18

2.4.4 基于网关的模型 18

2.4.5 基于令牌的模型 19

2.4.6 几种单点登录模型的比较 20

2.5 其他相关技术 21

2.5.1 Web Services 21

2.5.2 SOAP 协议 21

2.5.3 WSDL 22
2.5.4 UDDI 23
2.6 本章小结 24
第三章 几种身份认证方式的分析 25
3.1 Kerberos 协议 25
3.2 SAML 协议 27
3.3 Passport 协议 29
3.4 几种协议的安全性分析 31
3.4.1 Kerberos 安全性分析 31
3.4.2 SAML 安全性分析 32
3.4.3 Passport 安全性分析 33
3.5 本章小结 33
第四章 系统的设计与实现 34
4.1 系统设计原则 34
4.2 系统设计目标 35
4.3 系统的层次结构 36
4.4 身份认证系统的设计 37
4.4.1 系统的总体框架 37
4.4.2 用户身份认证 40
4.5 身份认证系统的实现 43
4.5.1 目录服务的实现 43
4.5.2 系统的部署 49
4.5.3 系统的运行情况 52
4.6 系统的特点 55
4.6.1 平台特性 55
4.6.2 功能特点 55
4.7 本章小结 56
第五章 总结与展望 57
5.1 总结 57

5.2 展望 57
参考文献 58
致谢 60

Contents

Chapter 1 Introduction 1

1.1 Background and Meaning of Thesis 1

1.2 Up-to-date Research Both Here and Abrord 2

1.3 Content and Structure of Thesis 3

Chapter 2 Relevant Techniques of Identity Authentication 5

2.1 Cryptology 5

2.1.1 Symmetric Key Algorithm 6

2.1.2 Asymmetric Key Algorithm 7

2.1.2 Other Cryptographic Algorithm 8

2.2 Identity Authentication 9

2.2.1 Identity Authentication Definition 9

2.2.2 Authentication Definition Methods 9

2.2.3 Authentication Definition Signification 12

2.3 LDAP Protocol 12

2.3.1 Overview of LDAP 12

2.3.2 Four Basic Model of LDAP 13

2.3.3 LDAP Security 15

2.3.4 Characteristic and Advantage of LDAP 15

2.4 Several Typical Single Sign On Model 16

2.4.1 Broker-Based Model 17

2.4.2 Agent-Based Model 18

2.4.3 Agent and Broker-based Model 18

2.4.4 Gateway Model 18

2.4.5 Token Model 19

2.4.6 Compare of Several SSO Model 20

2.5 Other Relevant Techniques 21

2.5.1 Web Services 21

2.5.2 SOAP Protocol 21

2.5.3 WSDL 22
2.5.4 UDDI 23
2.6 Summary 24
Chapter 3 Analysis and Compare of Several Identity Authentication 25
3.1 Kerberos Protocol 25
3.2 SAML Protocol 27
3.3 Passport Protocol 29
3.4 Security Analysis of Several Protocol 31
3.4.1 Safety Analysis of Kerberos 31
3.4.2 Safety Analysis of SAML 32
3.4.3 Safety Analysis of Passport 33
3.5 Summary 33
Chapter4 Design and Implementation of System 34
4.1 Principle of System Design 34
4.2 Goal of System Design 35
4.3 hiberarchy of System 36
4.4 Design of Identity Authentication System 37
4.4.1 Overall Architecture of Design 37
4.4.2 Identity Authentication 40
4.5 Implementation of Identity Authentication System 43
4.5.1 Implementation of Directory Services 43
4.5.2 Deployment of System 49
4.5.3 Operation of System 52
4.6 Characteristic of System 55
4.6.1 Speciality of Platform 55
4.6.2 Characteristic of Function 55
4.7 Summary 56